



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/306,110	05/06/1999	SATOSHI HASEGAWA	P/2850-19	3039
7590	11/25/2003		EXAMINER	
Dicksein Shapiro Morin & Oshinsky LLP 1177 Avenue of the Americas NEW YORK, NY 10036-2714			VAUGHAN, MICHAEL R	
			ART UNIT	PAPER NUMBER
			2131	9
			DATE MAILED: 11/25/2003	

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/306,110	HASEGAWA, SATOSHI
	Examiner	Art Unit
	Michael R Vaughan	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 21 October 2003.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-14 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-14 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 21 October 2003 is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

1. Certified copies of the priority documents have been received.

2. Certified copies of the priority documents have been received in Application No. _____.

3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) The translation of the foreign language provisional application has been received.

14) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) Notice of References Cited (PTO-892)

2) Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) Information Disclosure Statement(s) (PTO-1449) Paper No(s) 4.

4) Interview Summary (PTO-413) Paper No(s). _____.

5) Notice of Informal Patent Application (PTO-152)

6) Other: _____.

Detailed Action

The communication filed on 10/21/03 amended the specification and the drawings. Claims 1-14 are pending.

Response to Argument

Regarding Claim 1, applicants argue: *"Claim 1 is directed to a data transmission system that includes calculation means for performing calculation using a variable on an original data stream read from a recording medium so as to produce a calculated data stream; variable creation means for creating the variable; a stream buffer for temporarily storing the calculated data stream therein; inverse calculation means for performing inverse calculation on the calculated data stream output from the stream buffer to reproduce the data stream; stream processing means for processing the reproduced data stream to produce a processed data stream; and output means for outputting the processed data stream.*

The Office Action cited Hutter as teaching a stream buffer, stream processing means, and output means. However, the Office Action recognized that Hutter contains no teaching of means to perform calculations, inverse calculations or create variables, as recited, for example, in claim 1. In an attempt to remedy this deficiency, the Office Action relies upon Becker.

Hutter relates to a method whereby music CD reproduction can be enhanced when such a CD is played in a DVD player. The enhancement takes advantage of the fact that unlike a regular CD player, a DVD player has sufficient processing capability to perform more complex error correction on CD's played on the DVD player. By virtue of the DVD's hardware, increased error correction can be achieved without the necessity of additional, and costly, hardware.

The process of error correction of CD's does not require encryption and decryption techniques as described in Becker or the calculation, inverse calculation, and variable creation features of claim 1. Thus, there would have been no motivation whatsoever for one to have modified Hutter in the manner proposed in the Office Action. What would have been the point to have added the elements corresponding to the limitations missing from Hutter? Those elements would have been of no use at all in error correction of

CD's. The mere fact that a modification could have been is not sufficient to justify a rejection based on such a modification. There must be some motivation in the prior art that would have caused someone to have actually made the modification of the primary reference. In this case, no one would have made the proposed modification because it would have simply added useless hardware components to the DVD player.

In light of the foregoing, the only conceivable motivation to tack on features useless to the DVD player of Mutter is the need to meet the claim features. And of course this is not a proper motivation. Accordingly, the rejection amounts to an improper hindsight reconstruction of the claims and fails to set forth a prima facie case of obviousness. Accordingly, withdrawal of the rejection of claim 1 is respectfully requested. The other independent claims recite similar features and are believed patentable for similar reasons."

Examiner respectfully disagrees with applicants. All of the limitations set forth in claim 1 are met by the prior art teachings of Hutter in view of Becker. Hutter and Becker are without a doubt analogous art. In response to the lack of motivation the examiner supplies the motivation as taught by Becker in column 1, lines 13-18. This motivation is taught by Becker and is not an improper hindsight reconstruction of the claims. Becker clearly teaches that it is important for electronic data processing systems, which are used to a considerable extent to provide data privacy and protection against unauthorized use. Furthermore, Becker teaches that it is known to provide enciphering systems at those points of the system, which are particularly liable to unauthorized access. Becker's enciphering system protects data at liable points. One such liable point is memory. It is well known in the art that reading memory (a place for temporarily storing data) is a fundamental computer process and can be read from by simple instructions. Therefore, one skilled in the art would be motivated to protect the memory of electronic data processing systems, i.e. DVD players by the methods taught by Becker. Becker goes on to teach:

enciphering (calculating) data using a key or keys (variable) (column 18, lines 36-40);

deciphering (inverse calculating) (column 18, lines 55-58);

enciphering key generation (variable creation means) (column 2, lines 60-66).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to employ the teachings of Becker within the system of Hütter because protecting the data written into and read of out a buffer is imperative to the overall security of the device. Becker teaches a method in which data that is not meant to be freely distributed can be protected in an electronic device. DVD players, hard drives, and other medias that store data operate on data that is meant to be kept secret. These devices have memory buffers that temporarily hold the secret data. Therefore, protecting the memory buffers is advantageous to electronic data processing systems.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 3, 5, 8, 9, are rejected under 35 U.S.C. 103(a) as being unpatentable over Hütter (USP 6,160,785) in view of Becker (USP 4,157,454).

As per claim 1, Hütter teaches a data transmission system comprising:

a stream buffer (column 4, lines 11-12);

stream processing means (column 4, 22-23);

output means (column 4, 22-23). Hütter's art teaches the process of reading from a digital stored medium, to place that data into a buffer until it can be processed, and then outputted. Hütter is silent in disclosing a means to perform calculations, inverse calculations, and creating variables. Becker teaches:

Art Unit: 2131

enciphering (calculating) data using a key or keys (variable) (column 18, lines 36-40);

deciphering (inverse calculating) (column 18, lines 55-58);

enciphering key generation (variable creation means) (column 2, lines 60-66).

Becker also discloses that it is well known to provide enciphering systems at those points of the system which are particularly liable to unauthorized access (column 1, lines 13-18). One such liable point is memory. It is well known in the art that reading memory (a place for temporarily storing data) is a fundamental computer process. Therefore, it would be obvious to one in the art that if you want to protect memory from being read you should encipher it. Becker's cipher method is one way to protect memory.

In view of this, it would have been obvious to one in the art at the time of this invention to use an enciphering method to protect the buffer (memory) of Hütter's data transmission system.

As per claim 3, Becker teaches that one can implement a programmable logic array, PLA, which is known in the art, to cause random changes in the enciphering keys (column 17, lines 51-56). This would add increased safety. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to change the variables (keys) at arbitrary times. Clearly, the motivation is to increase the overall security of the calculation means.

As per claim 5, Hütter is silent in disclosing creating multiple keys. Becker teaches creating a number of keys (column 3, lines 1-13). Having multiple keys gives the calculator choice as to which variable (key) to use in calculating the input data. This choice further increases the security of the system. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to create multiple variables (keys).

As per claim 8, the examiner supplies the same rationale for the motivation as recited in rejection of claim 1. In addition, Hütter is silent in disclosing a means for creating multiple keys. Becker teaches creating a number of keys (column 3, lines 1-13). Having multiple keys gives the calculator choice as to which variable (key) to use in calculating the input data. This choice further increases the security of the system. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to create multiple variables (keys). Furthermore, Hütter is silent in disclosing modification modes. Becker teaches that modification modes (variable change codes) result in the changing of keys

Art Unit: 2131

(variables) (column 2, lines 53-55). Modification modes are signals to let the system know when a change of keys (variables) is taking place. Sending a modification mode signals that a change in keys has occurred. The absence of a modification mode signifies to continue to use the current key. This is a necessary function because the inverse calculator would not know when to use its new variable to decipher future data. The inverse calculator needs to know which variable to use to successfully decipher the data. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to use variable change codes to notify the inverse calculator of a change in variables.

As per claim 9, Hütter is silent in disclosing a changing the variable after each cycle. Becker teaches changing the variable after each enciphering operation (cycle) (column 2, lines 53-55). Clearly, the motivation is to increase the overall security of the system. Changing the variable after each cycle greatly increases the work necessary to one trying to compromise the system. The more ways you encipher data, the more ways one has to decipher them. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to change variables after each enciphering cycle to make the system more resistant to unauthorized deciphering.

As per claim 10, the examiner supplies the same rationale for the motivation as recited in rejection of claim 3.

Claims 2 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hütter and Becker as applied to claims 1 and 5 above, and further in view of Hanson (USP 5,132,955).

As per claim 2, the combination of Hütter and Becker are silent in disclosing the amount of data read into the buffer. Hanson's clearly suggests that buffer overflows should be prevented. He teaches that adjusting the speed of the CD can prevent buffer overflow (column 5, lines 19-23). Knowing at what rate to read data is directly proportional to the rate at which the data can be processed. If more data is read into the buffer than the processor can handle, a buffer overflow will occur. This is notoriously known in the art. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to input only an amount of data, which can be processed at a time.

As per claim 6, the examiner supplies the same rationale for the motivation as recited in rejection of claim 2.

Claims 4, 7, 11-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hütter and Becker as applied to claims 1-3, 5, 6, and 10 above, and further in view of Kato et al (US Patent Application 10/035,311).

As per claim 4, Hütter and Becker are silent in disclosing how the deciphering means (inverse calculator) obtain new deciphering keys (variable change codes). Kato teaching the use of a master key and session keys to notify the deciphering means when the enciphering means (calculator) has changed keys (variable change code) (page 7, paragraphs 0110-0111). The enciphering means sends a new session key to the deciphering means, which it uses to decipher future data. It is obvious that the deciphering means needs to know how the data it is receiving has been enciphered, in order to correctly decipher it. Kato teaches how this can be done. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to pass a variable change code from the calculator to the inverse calculator. In the context of this invention, it is obvious that the code must travel from the calculator to the inverse calculator via the buffer because that is the only data path to connecting the two.

As per claims 7, 11-14, the examiner supplies the same rationale for the motivation as recited in rejection of claim 4.

Final Rejection

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Art Unit: 2131

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patent

6,570,989 Ohmori et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

MV
Michael R Vaughan
Examiner
Art Unit 2131


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100